VIRUSTOTAL

SUMMARY DETECTION DETAILS BEHAVIOR COMMUNIT

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Display grouped sandbox reports

DOCGuard	0	0	0	0	0	0
VirusTotal Jujubox	0	0	0	0	10	2
Zenbox						
CAPE Sandbox						

There are some sandboxes still analysing the file.

Activity Summary

Download Artifacts Full Reports Help

Detections

NOT FOUND

Mitre Signatures

NOT FOUND

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

8 OTHER

Network comms

1 DNS 1 IP

Network Communication

DNS Resolutions

acroipm2.adobe.com

IP Traffic

UDP 8.8.8.8:53

Memory Pattern Domains

ftp.ky.gov

www.ipswitch.com

Memory Pattern Urls

https://ftp.ky.gov/human.aspx?r=1270737220&orgid=8628&rd=1

https://ftp.ky.gov/human.aspx?r=2042609911&arg12=home

https://ftp.ky.gov/human.aspx?r=7653090108&arg12=account

https://ftp.ky.gov/human.aspx?r=7653090108&arg12=infotech

https://ftp.ky.gov/human.aspx?r=7653090108&transaction=signoff

https://ftp.ky.gov/human.aspx?r=9495012966&Arg12=msgattchview&Arg06=310914239&Arg07=285818965&A

https://ftp.ky.gov/human.aspx?r=9495012966&arg03=285940741&arg07=reply&arg12=secmsgcompose

https://ftp.ky.gov/human.aspx?r=9495012966&arg06=285857710&arg12=mailbox

https://ftp.ky.gov/human.aspx?r=9495012966&arg06=730axe5c57sdh79j&arg12=useredit

https://ftp.ky.gov/human.aspx?r=9495012966&arg06=q5dt6a7n5e3bv9jm&arg12=useredit

Behavior Similarity Hashes

DOCGuard	612f9ffdb94bb481bfe87b2320074c6a
VirusTotal Juj…	427502d6ee33884fabc0aefdb86f88a5

File system actions

Files Opened

- /agm.ini
- C:\Program Files (x86)
- C:\Program Files (x86)\Common Files
- C:\Program Files (x86)\Common Files\
- C:\Program Files (x86)\desktop.ini
- C:\Users
- C:\Users\<USER>\
- C:\Users\<USER>\AppData
- C:\Users\<USER>\AppData\Local
- C:\Users\<USER>\AppData\Local\Adobe\Acrobat\
- C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\IconCacheRdr65536.dat
- C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json
- C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\UserCache.bin
- C:\Users\<USER>\AppData\Local\Microsoft\Windows\Caches
- C:\Users\<USER>\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
- C:\Users\<USER>\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000017.db
- C:\Users\<USER>\AppData\Roaming
- C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\Privileged\DC\
- C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\Privileged\DC\JavaScripts\
- C:\Users\<USER>\AppData\Roaming\Adobe\CoreSync\plugins\livetype\r
- C:\Users\<USER>\AppData\Roaming\Adobe\CoreSync\plugins\livetype\r\
- C:\Users\<USER>\Desktop\desktop.ini
- C:\Users\<USER>\Downloads\
- C:\Users\<USER>\Downloads\2025-10-04-MoveIt-CHFS-DCBS-Amy-Perry-System-Shows-No-Hidden-Now-Commonwealth of Kentucky_ icreateupwardspirals@gmail.com.pdf

- C:\Users\azure
- C:\Users\desktop.ini
- C:\Windows\Fonts\staticcache.dat
- C:\Windows\SysWOW64\propsys.dll
- C:\Windows\System32\wshtcpip.dll
- C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14b
- C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.24483_none_2b200f664577e14b\Comc
- C:\Windows\WindowsShell.Manifest
- C:\Windows\system32\CRYPTSP.dll
- C:\Windows\system32\DUI70.dll
- C:\Windows\system32\DUser.dll
- C:\Windows\system32\KBDUS.DLL
- C:\Windows\system32\MSVCP140.dll
- C:\Windows\system32\Msftedit.dll
- C:\Windows\system32\PROPSYS.dll
- C:\Windows\system32\RpcRtRemote.dll
- C:\Windows\system32\SensApi.dll
- C:\Windows\system32\UxTheme.dll
- C:\Windows\system32\VCRUNTIME140.dll
- C:\Windows\system32\api-ms-win-core-file-l1-2-0.dll
- C:\Windows\system32\api-ms-win-core-file-l2-1-0.dll
- C:\Windows\system32\api-ms-win-core-localization-l1-2-0.dll
- C:\Windows\system32\api-ms-win-core-processthreads-l1-1-1.dll
- C:\Windows\system32\api-ms-win-core-timezone-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-conio-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-convert-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-environment-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-filesystem-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-heap-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-locale-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-math-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-multibyte-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-runtime-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-stdio-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-string-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-time-l1-1-0.dll
- C:\Windows\system32\api-ms-win-crt-utility-l1-1-0.dll

- C:\Windows\system32\api-ms-win-downlevel-shell32-l1-1-0.dll
- C:\Windows\system32\explorerframe.dll
- C:\Windows\system32\ieframe.dll
- C:\Windows\system32\msls31.dll
- C:\Windows\system32\mswsock.dll
- C:\Windows\system32\ntmarta.dll
- C:\Windows\system32\ole32.dll
- C:\Windows\system32\propsys.dll
- C:\Windows\system32\rsaenh.dll
- C:\Windows\system32\tzres.dll
- C:\Windows\system32\ucrtbase.DLL
- C:\Windows\syswow64\SHELL32.dll
- C:\Windows\syswow64\en-US\USER32.dll.mui
- C:\Windows\win.ini
- C:\agm.ini
- STORAGE#Volume#{6a389d38-9fe6-11f0-84ea-806e6f6e6963}#0000000000100000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
- STORAGE#Volume#{6a389d38-9fe6-11f0-84ea-806e6f6e6963}#0000000006500000#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
- \Device\Afd\Endpoint
- agm.ini
- c:\program files (x86)\
- c:\program files (x86)\adobe\acrobat reader dc\
- c:\program files (x86)\adobe\acrobat reader dc\reader
- c:\program files (x86)\adobe\acrobat reader dc\reader\
- c:\program files (x86)\adobe\acrobat reader dc\reader\ACE.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\AGM.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\AXE8SharedExpat.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\AcroApp\
- c:\program files (x86)\adobe\acrobat reader dc\reader\AcroApp\ENU\
- c:\program files (x86)\adobe\acrobat reader dc\reader\AcroApp\ENU\Viewer.aapp
- c:\program files (x86)\adobe\acrobat reader dc\reader\AcroRd32.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\AdobeXMP.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\BIB.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\CoolType.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\JavaScripts\

- c:\program files (x86)\adobe\acrobat reader dc\reader\acrord32.exe.3.Manifest
- c:\program files (x86)\adobe\acrobat reader dc\reader\acrord32res.dll
- c:\program files (x86)\adobe\acrobat reader dc\reader\plug_ins\
- c:\program files (x86)\adobe\acrobat reader dc\reader\plug_ins\EScript.api
- c:\program files (x86)\adobe\acrobat reader dc\reader\plug_ins\pi_brokers\
- c:\program files (x86)\adobe\acrobat reader dc\reader\plug_ins\weblink.api

Files Written

C:\Users\<USER>\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-251002233017Z-331.bmp

C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\TESTING

C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json

C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\UserCache.bin

C:\Users\<USER>\AppData\Local\Temp\A9182zffr_jbamhe_11k.tmp

C:\Users\<USER>\AppData\Local\Temp\A91epklnz_jbamhc_11k.tmp

C:\Users\<USER>\AppData\Local\Temp\A91m37eyu_jbamhf_11k.tmp

C:\Users\<USER>\AppData\Local\Temp\A9r14ob3_jbamhd_11k.tmp

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\915DEAC5D1E15E49646B8A94E04E470958C9BB89.crl

C:\Users\<USER>\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\DF22CF8B8C3B46C10D3D5C407561EABEB57F8181.crl

Files Deleted

C:\Users\<USER>\AppData\LocalLow\Adobe\Acrobat\DC\ReaderMessages-journal

C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\ACROBAT_READER_MASTER_SURFACEID

C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\DC_READER_LAUNCH_CARD

C:\Users\<USER>\AppData\Local\Temp\A9182zffr_jbamhe_11k.tmp

C:\Users\<USER>\AppData\Local\Temp\A91epklnz_jbamhc_11k.tmp

C:\Users\<USER>\AppData\Local\Temp\A91m37eyu_jbamhf_11k.tmp

C:\Users\<USER>\AppData\Local\Temp\A9r14ob3_jbamhd_11k.tmp

C:\Users\
<USER>\AppData\Roaming\Adobe\Acrobat\DC\JSCache\GlobSettings

Files Dropped

C:\Users\
<USER>\AppData\LocalLow\Adobe\Acrobat\DC\ConnectorIcons\icon-251002233017Z-331.bmp

C:\Users\
<USER>\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\Files\TESTING

C:\Users\
<USER>\AppData\Local\Adobe\Acrobat\DC\SOPHIA\Reader\SOPHIA.json

C:\Users\<USER>\AppData\Local\Adobe\Acrobat\DC\UserCache.bin

C:\Users\<USER>\AppData\Local\Temp\A9182zffr_jbamhe_11k.tmp

C:\Users\<USER>\AppData\Local\Temp\A91epklnz_jbamhc_11k.tmp

C:\Users\
<USER>\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\915DEAC5D1E15E49646B8A94E04E470958C9BB89.crl

C:\Users\
<USER>\AppData\Roaming\Adobe\Acrobat\DC\Security\CRLCache\DF22CF8B8C3B46C10D3D5C407561EABEB57F8181.crl

Registry actions

Registry Keys Opened

- HKEY_CLASSES_ROOT\AcroExch.Document.DC\shell\Open\command
- HKEY_CLASSES_ROOT\Software\Adobe\Acrobat\MURD
- HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\TrustManager\cTrustedSites\cTrustedForPV
- HKEY_CURRENT_USER\SOFTWARE\Adobe\Acrobat Reader\DC\TrustManager\iProtectedView
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION
- HKEY_CURRENT_USER\Software
- HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\ADM
- HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\ARMReqManager
- HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVAlert

HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVAlert\cCheckbox

Registry Keys Set

Gemini Summary

- SOFTWARE\Adobe\Acrobat Reader\DC\DLLInjection\bBlockDLLInjection
- Software\Adobe\Acrobat Reader\DC\ExitSection\bLastExitNormal
- Software\Adobe\Acrobat Reader\DC\SessionManagement\bNormalExit
- Software\Adobe\Adobe Acrobat\DC\DiskCabs\bForms_AdhocWorkflowBackup
- Software\Adobe\Adobe Acrobat\DC\DiskCabs\bJSCache_GlobData
- Software\Adobe\Adobe Acrobat\DC\DiskCabs\bJSCache_GlobSettings
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
- c1\bHasComments
- c1\bisADCFile

Registry Keys Deleted

HKEY_LOCAL_MACHINE\System\Acrobatviewercpp473

Process and service actions

Processes Created

c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043

Processes Terminated

c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043

Processes Tree

1352 - c:/program files (x86)/adobe/acrobat reader dc/reader/acrord32.exe /A pagemode=FullScreen /s /o 2025-10-04-MoveIt-CHFS-DCBS-Amy-Perry-System-Shows-No-Hidden-Now-Commonwealth of Kentucky_ icreateupwardspirals@gmail.com.pdf

- 3136 - c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043
- 3096 - c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043
- 2332 - c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043
- 1576 - c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043
- 1284 - c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043
- 2732 - c:\program files (x86)\adobe\acrobat reader dc\reader\acrocef_1\RdrCEF.exe --backgroundcolor=16514043

Synchronization mechanisms & Signals

Mutexes Opened

- Global\ARM Update Mutex
- Global\Acro Update Mutex

Modules loaded

Runtime Modules

- ADVAPI32.dll
- API-MS-WIN-Service-Management-L1-1-0.dll
- API-MS-WIN-Service-winsvc-L1-1-0.dll
- API-MS-Win-Core-LocalRegistry-L1-1-0.dll
- API-MS-Win-Security-LSALookup-L1-1-0.dll
- API-MS-Win-Security-SDDL-L1-1-0.dll
- AXE8SharedExpat.dll
- AdobeXMP.dll
- BIBUtils.dll
- C:\Windows\system32\cryptnet.dll

Highlighted actions

Calls Highlighted

- GetAdaptersAddresses
- GetTickCount
- GetTickCount64
- IsDebuggerPresent

Highlighted Text

- "1"
- "11.69 x 16.54 in"
- "39.5%"
- "Adobe Acrobat"
- "Commonwealth of Kentucky: icreateupwardspirals@gmail.com - Adobe Acrobat Reader (32-bit)"